

***NATIONAL MARINE FISHERIES SERVICE INSTRUCTION 32-103-01
JUNE 14, 2002***

***Information Management
Web Server Administration***

***NOAA FISHERIES WEB SERVER AND INTERNET WEB SITE ADMINISTRATION:
OPERATING PROCEDURES AND GUIDELINES***

NOTICE: This publication is available at: <http://www.nmfs.noaa.gov/directives/>.

OPR: F/CIO

Certified by: F/CIO (L. Tyminski)

Type of Issuance: Renewal

SUMMARY OF REVISIONS:

Signed _____
[Approving Authority name] Date
[Approving Authority title]

**NOAA Fisheries Web Server and Internet Web Site Administration:
Operating Procedures and Guidance
June 14, 2002**

Effective Date: June 14, 2002

Section 1. Purpose.

These procedures provide guidance and best management practices for implementing, maintaining, and using NOAA Fisheries Web servers and NOAA Fisheries Internet Web sites and other related services.

Section 2. Scope and Applicability.

This guidance applies to all Internet Web servers and Web sites developed, implemented and operated by NOAA Fisheries staff or contractors.

Section 3. Terms and Definitions.

Content owner - The person and organizational unit responsible for the content on a Web page.

Cookie - Data that a Web server causes to be placed on a user's hard drive (or equivalent) that can be read by a Web server.

Extranet - A Web server that uses the Internet protocol and the public telecommunications system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers, or other organizations. An extranet can be viewed as part of an organization's intranet that is extended to users outside the organization.

Hit - Refers to a single action on the Web server as it appears in the log file. A visitor downloading a single file is logged as a single hit, while a visitor requesting a Web page including two images registers as three hits on the server (one for the .html page, and two for the image files).

Home page - The Web page that is the highest level of a hierarchy of electronic documents accessible by the user with a Web browser.

Intranet - A Web server, belonging to an organization, that is accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Persistent cookie - A cookie that is intended to maintain information over more than one browser session.

Unique visitor - A visitor to a web site as determined by his/her Internet Protocol (IP) address and domain name (and, on non-government servers and sites, by “cookies”). Sometimes known as the “dot address,” the IP address is a 32-bit number that identifies each sender or receiver of information across the Internet. An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular server or workstation within that network.

Web bug - Any element on a Web page that is designed to collect information on the identity and activity of persons who access the Web site.

Webmaster - Every NOAA Fisheries Web site shall have a designated Webmaster who will administer the site in accordance with official policies and procedures.

Web page - Any computer file, document, or grouping of electronic text which can be addressed by a hypertext link and rendered for a user on his/her computer monitor. This includes any grouping of electronic text, graphics material, or data generated by a software application and displayed through the use of a Web browser.

Web site - A collection of Web pages with a home page, managed as a unit.

Web site owner - The organization (office or division) that manages a Web site. The Web site owner for a NOAA Fisheries Web site is always a contact point within NOAA Fisheries.

Web server - A computer which provides access using the hypertext transfer protocol for applications and documents. A home page functions as the entry point for each Web server.

Web server administrator - The designated individual responsible for Web server operations within an approved NOAA Fisheries IT administrative unit.

Section 4. Background and Need.

NOAA Fisheries strongly encourages using the World Wide Web to convey information quickly and efficiently on a broad range of topics relating to the agency’s mission, objectives, activities, policies and programs. The diversity of agency activities and an organizational structure serving distinct constituencies and natural resources are well served by multiple Web sites addressing national and regional needs, yet with navigational links to the Department of Commerce, NOAA, and NOAA Fisheries hierarchies. Consistent with other leadership responsibilities for public and internal communication, and directives from NOAA, the agency encourages flexibility and

creativity in using Web sites to meet growing needs for communication and outreach.

At the same time, however, critical needs have arisen for uniform NOAA Fisheries Web server and Web site administrative procedures. In addition to the Department's Web standards, policies and best practices, issues of security, agency representation, and accountability require standardization of management practices. Of greatest concern is the increasing incidence of cyberattacks that result in denial of service, Web site defacement, and computer viruses, all of which seriously hinder the public's accessibility to NOAA Fisheries Web servers and sites. Rectifying these security breaches continues to consume disproportionate information technology resources and impedes development of products and services that advance NOAA Fisheries' mission. This document identifies the procedures for implementing and maintaining Web servers and Web sites that currently exist as well as those that are to be incorporated into NOAA Fisheries Information Technology (IT) operations.

Section 5. Responsibilities and Procedures.

.01 Chief Information Officer (CIO). Responsibility for the NOAA Fisheries Web servers and Web sites resides with the agency's Chief Information Officer. The NOAA Fisheries CIO shall annually certify that all NMFS Internet Web servers and Web sites are registered with the NOAA CIO, and shall annually certify to the Department CIO that all agency Web sites comply with the Department's Internet Web standards and policies.

.02 IT support staff. The CIO is assisted in administering the agency's Web services by the Regional Information Technology Coordinators (RITCs), the Office Information Technology Coordinators (OITCs), IT Security Officer (ITSO) and local security contacts, and the Headquarters Webmaster.

.03 Generic requirements and guidelines for all Department of Commerce, NOAA, and NOAA Fisheries IT policies and standards should be followed. These may be found at:

The NMFS Intranet
<http://www.ossec.doc.gov/webresources/>
<http://www.ossec.doc.gov/cio/internetmemo.htm>
<http://www.noaanews.noaa.gov/stories/iq.htm>

.04 NOAA Fisheries Web servers.

a. The following procedure is used to implement a Web server:

1. The proposed Web server administrator will submit the following general Web server operations information to the CIO or his/her designee:

(a) Proposed name and location of Web server;

- (b) Proposed Web server contact name, telephone number, e-mail address;
- (c) Designated Web server administrator, RITC or OITC, and IT Security Officer;
- (d) Concurrences from programmatic management;
- (e) The specific NOAA Fisheries strategic planning objective, e.g., *Recover and maintain protected species populations*; or the administrative/management function, e.g., *grants administration*, that the Web server will help meet;
- (f) Evaluation of available existing NOAA Web servers: indicate why one of the existing NOAA Fisheries or NOAA servers cannot be used; a list of these servers, by region, is provided at:

The NMFS Intranet

- (g) Identification of the IT security plan number covering the proposed Web server.

2. The proposed Web server administrator will also provide the CIO or his/her designee the following security information:

- (a) A statement indicating that only needed protocols and services are enabled;
- (b) A statement indicating that all operational protocols and services are consistent with, and covered under, the appropriate NOAA IT Security Plan, and the Department of Commerce Web Standards, Policies, and Best Practices.
- (c) Detailed description of intrusion prevention and detection capabilities, including security hardware and software, e.g., firewalls and virus detection software; provisions for security training for Web server administrators; procedures, including schedule, for continued verification; and operations procedures and processes, including monitoring, back-ups and disaster recovery, and incorporation of the proposed Web server in a current Disaster Recovery Plan for NOAA Fisheries or another NOAA Line Office.
- (d) The CIO, or his/her designee, may request additional information or make recommendations to improve the maintenance and utility of the Web

server.

3. The CIO shall approve or disapprove the proposed Web server in writing with comments. The decision may be appealed to the Deputy Assistant Administrator for Operations.

4. Upon written approval of the NOAA Fisheries CIO, the proposed Web server administrator must register the proposed Web server with the NOAA CIO.

b. Maintenance of NOAA Fisheries Web servers.

1. Security breaches. Any disruption of service resulting from a cyberattack should be handled by the local web server administrator in conjunction with the NOAA Computer Incident Response Team and the NOAA Fisheries IT Security Officer. These officials will notify the pertinent Webmaster(s) and jointly evaluate the effect on other Web servers. They may recommend steps to mitigate or correct damage, including advising the administrators of the affected Web server(s) when it is safe to resume operations. In accordance with CIO protocols, the webmaster will maintain documentation on all such attacks, including corrective action taken.

2. Maintenance and monitoring. Any change in Web server operations (disruptions for maintenance or repair, expansion, decision to permanently or temporarily disable, etc.) should be reported to the pertinent Webmaster as soon as possible. Web server administrators are expected to closely monitor the server(s) for level of utilization, content, compliance with all pertinent directives and standards, and need for modifications. The RITCs and OITCs shall annually certify to the NOAA Fisheries CIO or his/her designee that all Web servers under their purview comply with the Department's applicable standards and policies. These may be found at:

The NMFS Intranet

<http://www.ossec.doc.gov/webresources/>

<http://www.ossec.doc.gov/cio/internetmemo.htm>

.05 NOAA Fisheries Web sites. The following procedure is used to implement a NOAA Fisheries Internet Web site:

a. Web site eligibility. The CIO encourages Regional Administrators, Science Center Directors and Office Directors to designate organizational units eligible to host agency Web sites, and to develop appropriate approval procedures for specific Web site

applications. Every site shall use the domain name “nmfs.noaa.gov” except when exempted by the CIO.

b. Information. The proposed NOAA Web site owner will first submit for approval the following information on the Web site to the pertinent Web server administrator, and then the RITC or OITC:

1. Proposed name and location of Web site;
2. Proposed Web site owner, telephone number, e-mail address;
3. Designated Web server administrator/Webmaster, RITC or OITC, and local IT security contact;
4. Concurrences from programmatic management;
5. The specific NOAA Fisheries strategic planning objective, e.g., *Recover and maintain protected species populations*; or the administrative/management function, e.g., *contract administration*, that the Web site will help meet;
6. Linkages to other Web sites, including Departmental, NOAA, NOAA Fisheries, other Federal or State agencies, or external sites (standards and guidance for required links are given in Section 5.03);
7. Evaluation of existing, similar NOAA Web sites: indicate, to the extent known, any and all NOAA Fisheries or NOAA Web sites that are similar in content to the proposed site, and explain how the proposed site will coordinate with, or complement, information on this site(s);
8. A statement indicating that all operational protocols and services are consistent with, and covered under, the NOAA IT Security Plan, and the Department of Commerce Web Standards, Policies, and Best Practices.

c. Approval. The pertinent RITC or OITC will, upon approving the proposed Web site, forward the application to the CIO or his/her designee for approval. These officials, as well as the Web server administrator, Headquarters Webmaster, and CIO, may request additional information or make recommendations to improve the appearance, maintenance and utility of the proposed Web site. The CIO shall approve or disapprove the proposed Web site in writing with comments. The decision may be appealed to the Deputy Assistant Administrator for Operations.

d. Maintenance of NOAA Fisheries Web sites.

1. Security breaches. Any Web site defacement, denial of service or other disruption resulting from a cyberattack should be immediately reported to the local web server administrator for appropriate action in conjunction with the NMFS Information Technology Security Officer and NOAA Computer Incident Response Team in accordance with section 5.04.b.1 . The Network Administrator will maintain documentation on all such attacks, including corrective action taken.
2. Maintenance and monitoring. Anticipated changes to Web site operations should be discussed with the pertinent RITC or OITC, who will determine the need for additional approvals. Web site owners are expected to ensure that the server administrator has put in place a process for intrusion detection and is closely monitoring the site for level of utilization, need for updating, and compliance with all pertinent directives and standards.

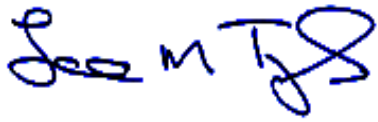
Section 6. References.

1. NOAA Administrative Order 212-13, Information Technology Security Management. <http://www.rdc.noaa.gov/~nao/212-13.html> and all referenced orders and guidance therein.
2. Department of Commerce Information Technology (IT) Restructuring Plan, Secretarial Directive, June 13, 2001.
3. NOAA Fisheries Web Guide
The NMFS Intranet
4. U.S. Department of Commerce Web Standards, Best Practices and Policies for Commerce Web sites
<http://www.osec.doc.gov/webresources/>
5. U.S. Department of Commerce, Information Technology Security Program
<http://www.osec.doc.gov/cio/oipr/ITSEC/DOC-IT-Security-Program-Policy.htm>
6. U.S. Department of Commerce Internet Use Policy
<http://www.osec.doc.gov/cio/internetmemo.htm>

Section 7. Effect on Other Issuances.

None

Signed,

A handwritten signature in blue ink, appearing to read "Law M TyS". The signature is stylized with a large "L" and a prominent "S" at the end.

Lawrence M. Tyminski
Chief Information Officer, NOAA Fisheries